Bases de Gröbner, à la rencontre entre géométrie algébrique et algorithmique

Thibaut Verron

sous la direction de Jean-Charles Faugère et Mohab Safey El Din

Table des matières

1 Introduction

La résolution de systèmes d'équations polynomiales est un problème récurrent en algèbre. Citons par exemple les vastes ramifications de la théorie des nombres, visant à résoudre les équations diophantiennes, c'est-à-dire les équations polynomiales dans l'anneau des entiers, ou encore la géométrie algébrique, qui étudie les ensembles de zéros d'idéaux polynomiaux. D'autre part, de nombreux problèmes extérieurs aux mathématiques font intervenir de telles équations. Ces problèmes peuvent apparaître par exemple

dans des théories scientifiques issues d'autres domaines, ou encore de questions tirées de la vie réelle, notamment en robotique ou en cryptographie.

L'enjeu des bases de Gröbner est de fournir un bon cadre pour résoudre ce genre de systèmes. Informellement, une base de Gröbner est un système de générateurs particulier d'un idéal, qui fournit donc une manière canonique de représenter cet idéal, et sur lequel on peut facilement lire des informations sur l'idéal.

Elles ont été inventées en 1965 par Bruno Buchberger, qui les a nommées d'après son directeur de thèse, Wolfgang Gröbner. Un concept similaire dans le cadre des anneaux locaux a été développé en 1964 par Heisuke Hironaka, sous le nom de base standard. La théorie a ensuite connu un essor grandissant dès les années 1990, lorsque les avancées technologiques ont permis de réaliser effectivement de plus en plus de calculs qui jusque là restaient théoriques. En particulier, l'article fondateur de Buchberger ne présentait qu'un algorithme, dit de Buchberger ([Buc76]). La recherche théorique a ensuite permis de développer de nouveaux algorithmes, comme par exemple les algorithmes F_4 ([Fau99]) et F_5 ([Fau02]), ou l'algorithme FGLM ([FGLM93]).

2 Ordres monomiaux et bases de Gröbner

Dans les algèbres de polynômes, un cas fait exception : c'est celui des polynômes en une seule indéterminée. Comme toutes les algèbres de polynômes, c'est une algèbre graduée, et cette graduation est une valuation qui en fait un anneau euclidien, et en particulier principal si l'anneau de base est un corps. Cette propriété fait qu'il existe une manière canonique de représenter tout idéal, et que l'on peut caractériser l'appartenance d'un polynôme à un idéal simplement en termes de divisions euclidiennes par ce générateur.

En général, une algèbre de polynômes en plusieurs indéterminées n'est ni euclidienne, ni principale. La graduation ne suffit pas à définir une valuation, notamment parce qu'il existe plusieurs monômes de même degré. L'idée sous-jacente aux définitions des bases de Gröbner est de copier le comportement des polynômes univariés, notamment en ce qui concerne la possibilité de « réduire un polynôme modulo un idéal ».

Pour cela, il faut commencer par définir un ordre sur les monômes, afin de pouvoir définir le *terme de tête* d'un polynôme.

Définition 1 (Ordre monomial admissible)**.** On appelle *ordre monomial admissible* toute relation d'ordre total sur l'ensemble des monômes de $k[X_1, \ldots, X_n]$ qui est compatible avec la multiplication, c'est-à-dire tel que pour tous monômes u, v et w, on a

$$(u \leq v \text{ et } w \geq 1) \implies uw \leq vw$$

Exemple 1. Voici deux exemples d'ordre monomiaux très utiles :

– l'ordre *lexicographique* Lex :

$$\mathbf{X}^\alpha <_{\text{lex}} \mathbf{X}^\beta \iff \exists 1 \leq i \leq n \begin{cases} \forall j < i, \alpha_j = \beta_j \\ \alpha_i < \beta_i \end{cases}$$

– l'ordre *lexicographique inversé en degrés* GRevLex (de l'anglais *graded-reverse lexicographical*) :

$$u <_{\text{grevlex}} v \iff \begin{cases} \deg(u) < \deg(v) \\ \text{ ou} \\ \deg(u) = \deg(v) \text{ et } u >_{\text{lex}} v \end{cases}$$

Définition 2 (Terme, monôme, coefficient de tête)**.** On se donne un ordre monomial sur $K[X_1, \ldots, X_n]$, pour tout $P \in K[X_1, \ldots, X_n]$, on définit :

– le *monôme de tête* de P, noté $\text{LM}(P)$, comme le plus grand monôme affecté d'un coefficient non nul dans P ;

– le *coefficient de tête* de P, noté $\text{LC}(P)$, comme le coefficient affecté à $\text{LM}(P)$;

– le *terme de tête* de P, noté $\text{LT}(P)$, comme le terme associé à $\text{LM}(P)$.

On peut à présent définir les notions de réduction modulo un ensemble de polynômes et de bases de Gröbner.

Définition 3. Soit $A = K[X_1, \ldots, X_n]$ un anneau de polynômes muni d'un ordre monomial $\prec$, et soit I un idéal de A. Soit P un ensemble de polynômes de A. On définit une opération de *réduction modulo* P par

$$f \xrightarrow[P]{} g \iff \exists p \in P, q \in A \text{ tels que } \begin{cases} f = pq + g \\ \text{LT}(g) < \text{LT}(f) \end{cases}$$

On dit que $f \xrightarrow[P]{*} g$ si et seulement s'il existe une suite de réductions modulo P de f à g, et on dit que f est *réduit modulo* P si et seulement s'il n'existe pas de réductions modulo P à partir de f.

Étant donnés deux polynômes f et g, on définit le *S-polynôme* de f et g par

$$\text{S-Pol}(f, g) = \frac{\text{LT}(f) \vee \text{LT}(g)}{\text{LT}(f)} f - \frac{\text{LT}(f) \vee \text{LT}(g)}{\text{LT}(g)} g$$

On dit qu'un ensemble de polynômes $G = \{g_1, \ldots, g_m\}$ de A est une *base de Gröbner* de I si et seulement si $\langle G \rangle = I$ et si de plus G vérifie l'une des conditions équivalentes suivantes :

i. l'idéal engendré par les termes de tête de G est égal à l'idéal engendré par les termes de tête de I

ii. pour tout polynôme P de I, $\text{LT}(P)$ est divisible par le terme de tête d'un des polynômes de G ;

iii. le S-polynôme $\text{S-Pol}(g_1, g_2)$ se réduit à 0 modulo G, pour toute paire (g_1, g_2) de polynômes de G ;

iv. l'opération de réduction itérée modulo G est confluente, c'est-à-dire que pour tout polynôme $P \in A$, il existe un unique polynôme Q tel que $P \xrightarrow[G]{*} Q$ et tel que Q est réduit modulo G.

Avec les notations de la condition (iv), on appelle *forme normale*, et l'on note NF la fonction qui à P associe Q. Par définition, cette fonction est telle que

$$\mathrm{NF}(P) = 0 \iff P \in I \tag{1}$$

Remarquons que la condition (iii) fournit un critère algorithmique pour vérifier qu'un système donné est une base de Gröbner.

Tout idéal admet une base de Gröbner, et il existe des algorithmes permettant de la calculer, étant donné un système de générateurs de l'idéal. De plus, si on impose de plus que la base soit *réduite*, c'est-à-dire qu'aucun des polynômes de la base n'est réductible par les autres, et que ces polynômes soient tous unitaires, la base de Gröbner ne dépend que de l'idéal considéré et de l'ordre monomial choisi.

Concluons cette section par le rappel de quelques définitions issues de l'algèbre commutative et de la géométrie algébrique . Soit K un corps, on appelle *K-espace affine de dimension n* l'ensemble $\mathbb{A}^n_K := K^n$. On appelle *variété algébrique affine* toute partie de $\mathbb{A}^n_K$ qui peut être décrite comme le lieu des zéros communs d'une famille de polynômes. L'ensemble des variétés algébriques forme les fermés d'une topologie sur $\mathbb{A}^n_K$, appelée *topologie de Zariski*. La *dimension* d'une variété algébrique est définie comme sa dimension de Krull pour cette topologie.

3 Influence du choix de l'ordre

Comme on l'a vu, la définition d'une base de Gröbner dépend du choix d'un ordre monomial. Ce choix est loin d'être anodin : différents ordres donneront différentes bases, et ces bases vérifieront différentes propriétés. D'autre part, certains ordres donnent des bases qui n'ont que peu de propriétés, mais qui s'avèrent bien plus faciles à calculer en général que les bases pour les ordres riches en propriétés.

L'ordre lexicographique : un ordre d'élimination

On va commencer par présenter un exemple de propriété recherchée pour les bases de Gröbner, appelée *propriété d'élimination*.

Théorème 4 (Propriété d'élimination pour l'ordre lexicographique)**.** *Soit I un idéal de $K[X_1, \ldots, X_n]$. Soit G une base de Gröbner de I pour l'ordre* Lex *avec $X_1 > \cdots > X_n$. Alors cette base de Gröbner satisfait la* propriété d'élimination*, c'est-à-dire que*

$$I \cap K[X_k, \ldots, X_n] = \langle G \cap K[X_k, \ldots, X_n] \rangle$$

Cette propriété permet comme son nom l'indique d'*éliminer* des inconnues du système.

On peut par exemple l'utiliser pour résoudre un système d'équations polynomiales n'ayant qu'un nombre fini de solutions. En effet, considérons le système

$$\begin{cases} f_1(X_1, \ldots, X_n) &= a_1 \\ & \vdots \\ f_n(X_1, \ldots, X_n) &= a_n \end{cases}$$

et supposons-le de dimension nulle.

On calcule une base de Gröbner de $\langle f_1 - a_1, \ldots, f_n - a_n \rangle$ pour l'ordre Lex $X_1 > \cdots > X_n$. Si le système n'a qu'un nombre fini de solutions, il existe dans cet idéal un polynôme qui ne fait apparaître que X_n, et ainsi, par propriété d'élimination, il existe dans la base de Gröbner un polynôme g_1 qui ne fait intervenir que X_n. En itérant le processus, on montre que la base de Gröbner a une structure d'*escalier* comme ci-dessous :

$$\begin{cases} g_1 &\in K[X_n] \\ g_2 &\in K[X_{n-1}, X_n] \\ & \vdots \\ g_n &\in K[X_1, \ldots, X_n] \end{cases}$$

Pour trouver une solution du système, il suffit alors de résoudre g_1, de choisir une de ses solutions z_n, puis de résoudre $g_2(X_n := z_n)$ (polynôme univarié en X_{n-1}), et ainsi de suite jusqu'à g_n. On trouve ainsi que le point $(z_1, \ldots, z_n)$ est une solution du système, en n'ayant à résoudre que des équations polynomiales à une seule inconnue.

On peut également utiliser cette propriété pour convertir une définition paramétrique d'une variété en une définition non paramétrique. Soit

$$\begin{cases} X_1 &= f_1(T_1, \ldots, T_m) \\ X_2 &= f_2(T_1, \ldots, T_m) \\ & \vdots \\ X_n &= f_n(T_1, \ldots, T_m) \end{cases}$$

On calcule une base de Gröbner de $\langle X_1 - f_1, \ldots, X_n - f_n \rangle$ pour l'ordre Lex avec $T_1 > \cdots > T_m > X_1 > \cdots > X_n$. En ne conservant que les polynômes de la base de Gröbner qui ne contiennent pas de T_i, on obtient une définition non paramétrique de la plus petite variété affine contenant notre ensemble de départ.

Cette propriété d'élimination permet également de calculer diverses manipulations d'idéaux utiles en géométrie algébrique, comme l'idéal intersection ou l'idéal colonne de deux idéaux. Pour plus de détails (et d'autres applications), on pourra se référer à [CLO07].

L'ordre GRevLex, un ordre pour des calculs plus faciles

Lorsqu'on effectue des calculs de bases de Gröbner, on est amenés à faire différents choix. Informellement, les différents algorithmes reviennent tous à étudier une liste de

polynômes de l'idéal que l'on considère, et à les réduire entre eux jusqu'à avoir une base. À chaque étape, il faut donc choisir quelle réduction on va effectuer, et c'est sur ce choix que se fait principalement la distinction entre les différents algorithmes.

Il apparaît, expérimentalement, que le critère « on réduit en priorité les polynômes de plus bas degré » permet d'accélérer fortement les calculs, et c'est le critère utilisé par les algorithmes F_4 et F_5, qui sont les algorithmes les plus rapides à ce jour. De plus, ce phénomène est encore accentué lorsqu'on choisit un ordre raffinant l'ordre du degré, tel l'ordre GRevLex.

Cependant, l'ordre GRevLex n'est pas un ordre d'élimination. Pour pouvoir tout de même profiter de ces observations, on a développé des algorithmes dits de *changement d'ordre*, comme l'algorithme FGLM ([FGLM93]) en dimension nulle : il prend en entrée une forme normale, c'est-à-dire une fonction NF vérifiant la condition (1), et s'en sert pour construire une base de Gröbner Lex de l'idéal ker(NF). Une stratégie de calcul courante consiste alors à procéder en deux étapes :

1. calculer avec l'algorithme F_5 une base de Gröbner G' de l'idéal pour l'ordre GRevLex, et la forme normale NF associée ;
2. appliquer l'algorithme FGLM à la forme normale NF pour obtenir une base de Gröbner Lex de l'idéal.

Cet algorithme s'avère généralement plus rapide qu'un calcul direct.

4 Calculs de complexité

Complexité au pire ou générique

La complexité des algorithmes précédents est connue :

Théorème 5. *Soit F un système de polynômes en n indéterminées, de dimension nulle. On note D le* degré *du système, défini comme son nombre de solutions comptées avec multiplicité, et d_{reg} son degré de régularité, défini comme le plus haut degré d'un polynôme considéré par l'algorithme F_5 sur ce système (en particulier, d_{reg} est supérieur au degré des polynômes de la base de Gröbner* GRevLex *calculée). Alors la complexité du calcul d'une base* Lex *pour ce système est en*

$$O\left(d_{\text{reg}}\binom{n+d_{\text{reg}}-1}{d_{\text{reg}}}^3 + nD^3\right).$$

Les valeurs de cette complexité *dans le pire des cas* sont indépendantes de l'ordre utilisé, et données par le théorème suivant, prouvé par exemple dans [BS88].

Théorème 6. *Pour tout corps K, et tout entier D, il existe un système de n polynômes en n variables, tel que pour tout ordre monomial, la base de Gröbner de ce système contienne des polynômes de degré D^{2^n}, et le calcul de cette base se fait en temps polynomial en D^{2^n}.*

Cependant, ces pires cas sont des systèmes construits dans ce but précis, et n'apparaissent pas pour des calculs issus de la « vie réelle ».

On cherche donc plutôt à obtenir des résultats de complexité *générique*, c'est-à-dire valables sur une partie Zariski-dense de l'ensemble des systèmes, qui seront par exemple valides sur des systèmes pris au hasard. En pratique, cela revient à séparer la question de la complexité du calcul en deux problèmes indépendants :

- étant donné une propriété P des systèmes de polynômes, obtenir un résultat de complexité pour les systèmes vérifiant P ;
- montrer que la propriété P est générique.

Lorsqu'on cherche à évaluer la complexité d'un calcul de base de Gröbner pour un système vérifiant une propriété P, il n'est en général pas nécessaire d'étudier en détail le fonctionnement de l'algorithme. En effet, grâce au théorème 5, on constate qu'il suffit de recalculer le degré et le degré de régularité d'un système vérifiant P, et d'en déduire une nouvelle borne de complexité pour ces systèmes.

Concluons ce paragraphe en citant un outil majeur pour évaluer ces paramètres :

Définition 7. Soit I un idéal de $A = K[X_1, \ldots, X_n]$, on définit la *série de Hilbert* de A/I comme la série formelle

$$HS_{A/I}(t) = \sum_{d=0}^{\infty} c_d t^d$$

où c_d est la dimension, comme K-espace vectoriel, de l'ensemble des polynômes de A/I de degré d.

Son intérêt majeur vient de la propriété suivante :

Proposition 8. *Soit F un système engendrant un idéal de dimension nulle, HS sa série de Hilbert, D son degré et d_{reg} son degré de régularité. Alors*

- *$HS(t)$ est un polynôme en t ;*
- *$D = HS(t := 1)$;*
- *$d_{\text{reg}} \leq \deg(HS) + 1$.*

Un exemple de calcul de complexité : le cas des suites régulières

Un bon exemple de telle propriété est la régularité.

Définition 9. Une suite $f_1, \ldots, f_m$ de polynômes de $K[X_1, \ldots, X_n]$ est dite *régulière* si elle vérifie l'une des conditions équivalentes suivantes :

i) pour tout $i \in \{1, \ldots, m\}$, f_i n'est pas diviseur de 0 dans l'algèbre $K[X_1, \ldots, X_n]/\langle f_1, \ldots, f_{i-1}\rangle$;

ii) la dimension de l'idéal $\langle f_1, \ldots, f_m\rangle$ est égale à $n - m$;

iii) la série de Hilbert de l'idéal $\langle f_1, \ldots, f_m \rangle$ s'écrit

$$\begin{aligned} HS(t) &= \frac{(1-t^{d_1}) \cdots (1-t^{d_m})}{(1-t)^n} \\ &= \frac{(1+\cdots+t^{d_1-1}) \cdots (1+\cdots+t^{d_m-1})}{(1-t)^{n-m}}, \end{aligned}$$

où les d_i sont les degrés respectifs des polynômes f_i.

Géométriquement, définir une variété par une suite de polynômes peut être vu comme un processus itératif : à l'étape i, on dispose de la variété définie par $\langle f_1, \ldots, f_i \rangle$, et on « coupe » dans cette variété la « tranche » correspondant aux zéros de f_{i+1}. Dans ce cadre, la notion algébrique de suite régulière correspond à la notion géométrique d'*intersection complète* : une suite régulière est une suite pour laquelle ce processus correspond réellement à un découpage en tranches, c'est-à-dire qu'à chaque étape, on découpe réellement une variété de dimension inférieure.

Pour une suite régulière $(f_1, \ldots, f_n)$ de degrés $(d_1, \ldots, d_n)$, on a donc

$$\begin{aligned} D &= \prod_{i=1}^{n} d_i \\ d_{\text{reg}} &\leq \sum_{i=1}^{n} (d_i - 1) + 1 \end{aligned}$$

et on en déduit que la complexité du calcul d'une base de Gröbner Lex se fait en temps $O(d^{3n+1})$ où $d = \max\{d_i\}$.

Généricité et problèmes ouverts

Vérifier qu'une propriété est générique, c'est-à-dire Zariski-dense, n'est pas facile en général. Il est connu que pour la topologie de Zariski, tout ouvert non vide est dense, ce qui ramène la vérification à deux étapes :

- montrer que la propriété est *ouverte*, c'est-à-dire que les coefficients des systèmes qui ne la vérifient pas doivent annuler un certain ensemble d'équations polynomiales ;
- montrer que la propriété est *non vide*, c'est-à-dire que pour toute famille d'entiers D, il existe un système d'équations polynomiales de degrés respectifs D vérifiant la propriété.

Assez paradoxalement, la seconde étape s'avère souvent plus difficile à vérifier que la première.

Exemple 2. Quelques exemples de propriétés génériques (ou non) :

1. la propriété de régularité définie plus haut est générique ;

2. lorsqu'on étudie des systèmes issus par exemple de la cryptographie, il arrive souvent que l'on ait plus d'équations que d'inconnues. Le système est alors dit *surdéterminé*. Un tel système ne peut pas être régulier, mais il peut être *semi-régulier*, c'est-à-dire, par définition, que sa série de Hilbert s'obtient en tronquant

$$\frac{(1-t^{d_1})\cdots(1-t^{d_m})}{(1-t)^n}$$

au premier coefficient strictement négatif. À ce jour, la question de savoir si la propriété de semi-généricité est générique est encore ouverte. Plus précisément, il est connu que la condition est ouverte. En revanche, savoir si la condition est non vide fait l'objet d'une conjecture, formulée dans les années 1980 par Ralf Fröberg ([Frö82]).

En fait, expérimentalement, on constate que beaucoup de caractéristiques des idéaux et des bases de Gröbner semblent être invariantes pour tous les systèmes génériques. Par exemple, on peut définir l'*escalier* d'un idéal pour un ordre comme le complémentaire de l'ensemble des monômes de tête des polynômes de cet idéal pour cet ordre. Cet objet est une caractéristique importante de l'idéal, qui contient par exemple le degré de régularité. Il semblerait que l'escalier d'un système générique ne dépende que des degrés des polynômes du système, mais ce n'est pas démontré. Plus précisément, Guillermo Moreno-Socías a formulé en 2003 une conjecture portant sur une description précise de l'escalier d'un système générique ([MS03]), et cette conjecture a des implications importantes dans les calculs de bases de Gröbner et de leur complexité. Parmi ces conséquences, elle impliquerait notamment la conjecture de Fröberg.

L'autre aspect, à savoir trouver les propriétés qui garantissent de meilleurs résultats de complexité, fait également l'objet d'une recherche active. Selon la propriété considérée, cela peut s'avérer plus ou moins compliqué : cela dépend en fait à quel point la propriété est facile à transcrire de manière algébrique. Ainsi, l'étude de complexité pour un système régulier ou semi-régulier est relativement facile. En revanche, voici un exemple de propriété pour laquelle l'étude est compliquée : on observe expérimentalement que les calculs de base de Gröbner sont plus rapides sur des systèmes *creux* (où peu de monômes sont affectés d'un coefficient non nul) que sur des systèmes génériques. Mais à ce jour, trouver une explication à ce phénomène est une question en grande partie ouverte, la principale difficulté étant de formaliser algébriquement la propriété.

Le sujet de mon mémoire de M2, et celui vers lequel semble s'orienter ma thèse, concerne les systèmes polynomiaux quasi-homogènes, c'est-à-dire homogènes lorsque les indéterminées sont affectées d'un degré non nécessairement égal à 1. L'étude porte sur plusieurs points, notamment étudier les calculs de complexité pour ces systèmes, étudier et comparer différents algorithmes permettant de mener les calculs sur ces systèmes, ainsi que montrer que diverses propriétés, dont la généricité pour les systèmes homogènes est connue, restent génériques dans le cas quasi-homogène.

Références

[BS88] David Bayer and Michael Stillman. On the complexity of computing syzygies. *J. Symb. Comput.*, 6(2-3) :135–147, December 1988.

[Buc76] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3) :19–29, August 1976.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3) :61–88, June 1999.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international s ymposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[FGLM93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4) :329–344, 1993.

[Frö82] R. Fröberg. *An Inequality for Hilbert Series of Graded Algebras.* 1982.

[MS03] Guillermo Moreno-Socías. Degrevlex Grobner bases of generic complete intersections. *Journal of Pure and Applied Algebra*, 180 :263–283, 2003.